Exhibit 2

US9172629B1	Specification Support	F5 Networks – Big-IP Policy Enforcement Manager (The accused product)
1pre. A method for processing a packet, comprising: **1a.** determining if the packet is classified according to an attribute of a classification index, the classification index being a part of a set of one or more classification indices and said attribute includes a classification index valid bit; and	**Upon receiving a packet for classification, common classifier 604 reads information associated with the packet, such as from the packet header and/or body.** Such information may include, for example, protocol, source address, destination address, source port, destination port, source interface, destination interface, etc. [Col. 7, Line 35-40] **A set of unique classification outcomes may be stored and/or indexed in a table**. In the given example, a set of unique classification	The accused product practices a method for processing a packet, comprising determining if the packet is classified according to an attribute of a classification index, the classification index being a part of a set of one or more classification indices, and said attribute includes a classification index valid bit. F5 Networks, Inc. specializes in application services and application delivery networking (ADN). F5 technologies focus on the delivery, security, performance, and availability of web applications, including the availability of computing, storage, and network resources. F5 Networks provides BIG-IP products. F5's BIG-IP is a family of products covering software and hardware designed around application availability, access control, and security solutions. F5 BIG-IP Policy Enforcement Manager (PEM) delivers the insight a user needs to understand subscriber behavior and effectively manage network traffic with a wide range of policy enforcement capabilities. See Fig. 1. **Citation 1: F5 BIG-IP Policy Enforcement Manager (PEM)**  Fig. 1

Exhibit 2

	outcomes are stored and indexed in global classification table 614. Each indexed entry in global classification table 614 specifies a set of one or more rules that need to be satisfied to have that unique classification. [Col. 7, Line 47-52] In some embodiments, once a packet's unique classification has been determined, the **classification index associated with that classification is attached to the packet**. In some embodiments, the classification index is written into the packet context. In some embodiments, the	Source: https://www.f5.com/products/big-ip-services/policy-enforcement-manager, Page 1, Last accessed April 28, 2020, Exhibit C BIG-IP PEM dynamically manages traffic and subscribers in real-time to optimize QoE and minimize congestion in the network. See Fig. 2. **Citation 2: F5 BIG-IP Policy Enforcement Manager (PEM) Introduction** F5® BIG-IP® Policy Enforcement Manager™ (PEM) delivers the insight you need to understand subscriber behavior and effectively manage network traffic with a wide range of policy enforcement capabilities. BIG-IP PEM provides intelligent layer 4–7 traffic steering, network intelligence, and dynamic control of network resources through subscriber- and context-aware solutions. It also provides deep reporting, which you can capitalize on to build tailored services and packages based on subscribers' app usage and traffic classification and patterns to increase ARPU. Fig. 2 Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 1, Last accessed April 28, 2020, Exhibit A The PEM performs deep packet inspection (i.e., processing a packet). See Fig. 3.

Exhibit 2

	classification index is written into the packet header. [Col. 7, Line 59-65] In some embodiments, **the validity of a classification index of a packet is managed via a "classification index valid' bit of the packet. Such as bit may be a part of the packet header, packet context flags field, etc. For example, if the classification index valid bit is set, the classification index associated with the packet may be considered to be valid and may be used by a node processing the packet. However, if the**	**Citation 3: PEM's deep packet inspection** Other types of traffic classification employed on BIG-IP PEM include behavior and heuristics analysis, and deep packet inspection. Fig. 3 Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, Last accessed April 28, 2020, Exhibit A BIG-IP PEM provides intelligent traffic steering, network intelligence, and dynamic control of network resources through subscriber and context-aware solutions. BIG-IP PEM makes the IP devices subscriber aware. The subscriber's data does not pass through an IP device anonymously. When BIG-IP PEM is operating, the address of a data packet for a subscriber that is passing through the device is mapped to a subscriber's identity (i.e., the classification index). See Fig. 4.

Exhibit 2

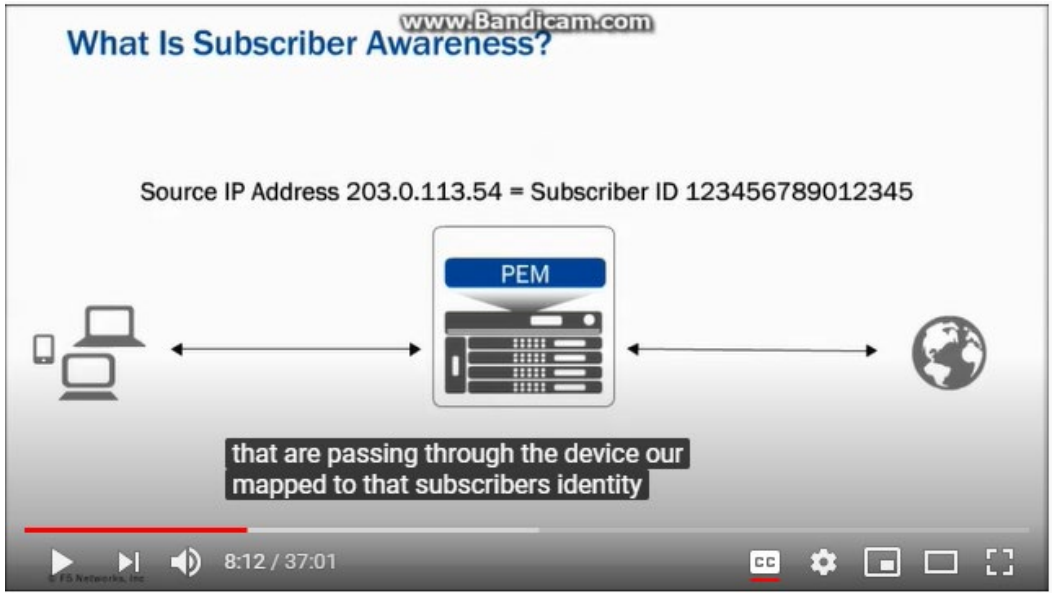
	classification index valid bit is clear, the classification index associated with the packet may be considered to be invalid or obsolete, and the packet may need to be reclassified. In some embodiments, whenever a packet is classified, the valid bit is set. In some embodiments, 810 of FIG. 8 includes setting the valid bit. [Col. 9, Line 50-62]	**Citation 4: Subscriber Awareness**  Fig. 4 Source: https://www.youtube.com/watch?v=HxzI2BKy_jg, Timestamp 8:12/37:01, Last accessed April 28, 2020, Exhibit B Different policies are assigned to a subscriber, ultimately to the subscriber ID (i.e., the classification index), based on the user requirement. E.g., one user may want higher bandwidth, while other user wants some parental control. Therefore, packets are mapped to a subscriber's identity (Subscriber ID) (i.e., classification index). Further processing on the packet is based on the subscriber's ID associated with it. As an example,

Exhibit 2

		'Global_BWC_Policy' has been applied to the subscriber having ID as '123456789012345'. Whenever a packet for this subscriber arrives at the PEM, it will be mapped with the subscriber's ID, and further processing on the packet will be done based on rules defined in the policies associated with the subscriber. See Fig. 5. **Citation 5: Applying a policy to a subscriber**  Fig. 5 Source: https://www.youtube.com/watch?v=HxzI2BKy_jg, Timestamp 36:13/37:01, Last accessed April 28, 2020, Exhibit B

Exhibit 2

		BIG-IP PEM allows to configure enforcement policies. An enforcement policy is a set of rules that determine what to do with specified types of traffic. It is made of a set of rules and the rules define a condition and an action on what to do when the system receives a particular type of traffic. See Fig. 6. **Citation 6: Enforcement policies in BIG-IP PEM** **About enforcement policies** An ***enforcement policy*** is a set of rules that determines what to do with specified types of traffic. You can configure policies on the BIG-IP® system using Policy Enforcement Manager™ (PEM), or receive policy definition from a PCRF. **About enforcement policy rules** An enforcement policy is made up of a set of rules. In the policy, rules define what to do when the system receives a particular type of traffic. There are many ways you can set up a rule so that you can handle the traffic exactly as you need to. Each rule includes a condition and an action. Fig. 6 Source: https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-13-0-0/1.html#guid-ee75a1d4-4c4d-4faf-a986-d22118411e0e, Page 1-2 , Last Accessed September 3, 2020, Exhibit D As per the patent specification, "*A rule or policy definition may be based on packet parameters such as protocol, Source address, destination address, source port, destination port, Source interface, destination interface, etc., and/or one or more lists of such parameters.*" [Col. 6, Line 40-44]. A rule in an enforcement policy defines the conditions that the traffic must meet (or not meet) for the rule to apply. The rule conditions fall into the following criteria: Classification criteria, Flow information, URL information and Custom criteria. BIG-IP PEM allows to classify traffic based

Exhibit 2

		on the flow information criteria specifies the traffic associated with specific source and destination IP addresses or ports. See Fig. 7. **Citation 7: Rules in BIG-IP PEM** A rule defines conditions that the traffic must meet (or not meet) for the rule to apply. The conditions fall into the following criteria: • ***Classification criteria***, such as applications or categories of applications that the system detects. For example, a rule can apply to all webmail traffic or to a specific webmail application. • ***Flow information***, such as traffic associated with specific source and destination IP addresses or ports, or incoming DSCP marking. For example, a rule can apply to all traffic directed to a specific destination port. • ***URL information***, such as URL categories that the system detects. For example, the rule may categorize adult traffic and prevent access to it. • ***Custom criteria***, which are other conditions that you develop using iRules® Fig. 7 Source: https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-13-0-0/1.html#guid-ee75a1d4-4c4d-4faf-a986-d22118411e0e, Page 2 , Last Accessed September 3, 2020, Exhibit D The rule specifies actions to take when the set criteria in the rule is met by the traffic. Some of the actions a rule can take is shown in Fig. 8. **Citation 8: Actions taken by rules** If the traffic meets the criteria in the rule, the rule specifies actions to take, such as: • Dropping traffic • Forwarding traffic to a specific endpoint or series of endpoints for value-added services • Redirecting HTTP traffic to a URL • Generating reporting data for further processing by external analytic systems • Usage monitoring about the traffic to the PCRF so it can track mobile usage. • Setting DSCP bits in the IP header of the traffic by marking all or marking upon the traffic exceeding a threshold • Setting Layer 2 Quality of Service (QoS) levels for the traffic • Enforcing rate control using a bandwidth control policy Fig. 8

Exhibit 2

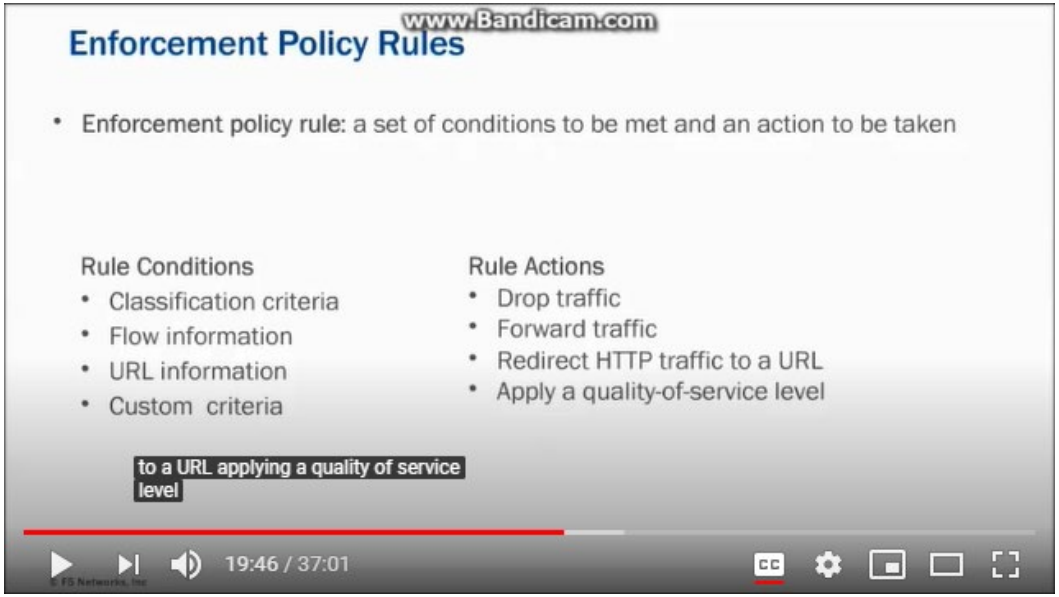
		Source: https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-13-0-0/1.html#guid-ee75a1d4-4c4d-4faf-a986-d22118411e0e, Page 2, Last Accessed September 3, 2020, Exhibit D Fig. 9 shows different rule conditions to be met and different rule actions taken by the corresponding nodes. **Citation 9: Enforcement Policy Rules**  Fig. 9 Source: https://www.youtube.com/watch?v=HxzI2BKy_jg, Timestamp 19:46/37:01, Last accessed April 28, 2020, Exhibit B

Exhibit 2

		The packets are classified based on the rules (i.e., Attributes) associated such as classification criteria, flow information, URL information, etc. with the subscriber's ID (classification index). For identifying a packet for a user, the subscriber ID is in use. If the corresponding packet gets processed by the destination node, then it will be considered as a valid classification (i.e. classification index valid bit is set). Note: Further Search/ Source Code Review/ Product Testing could help in gathering additional evidence related to the claim limitation "*determining if the packet is classified according to an attribute of a classification index, the classification index being a part of a set of one or more classification indices and said attribute includes a classification index valid bit. "*
1b. using, when the packet has been classified, the classification data of the packet to determine a node-specific policy of the receiving node applicable to the packet, wherein a plurality of node-specific policies associated with a plurality of nodes is specified using the classification data, the plurality of nodes including the receiving	A rule or policy may be defined by a basic packet matching specification**. A rule or policy definition may be based on packet parameters such as protocol, Source address, destination address, source port, destination port, Source interface, destination interface, etc.,** and/or one or more lists of such parameters. Moreover, a	The method practiced by the accused product comprises using, when the packet has been classified, the classification data of the packet to determine a node-specific policy of the receiving node applicable to the packet, wherein a plurality of node-specific policies associated with a plurality of nodes is specified using the classification data, the plurality of nodes including the receiving node, wherein at least two of the plurality of node-specific policies are different, and wherein the at least two node-specific policies are associated with respective at least two different nodes of the plurality of nodes. Different policies, such as predefined policies, custom policies can be assigned to a subscriber. A data packet is further processed based on these policy rules (i.e., the classification data). See Fig. 10.

Exhibit 2

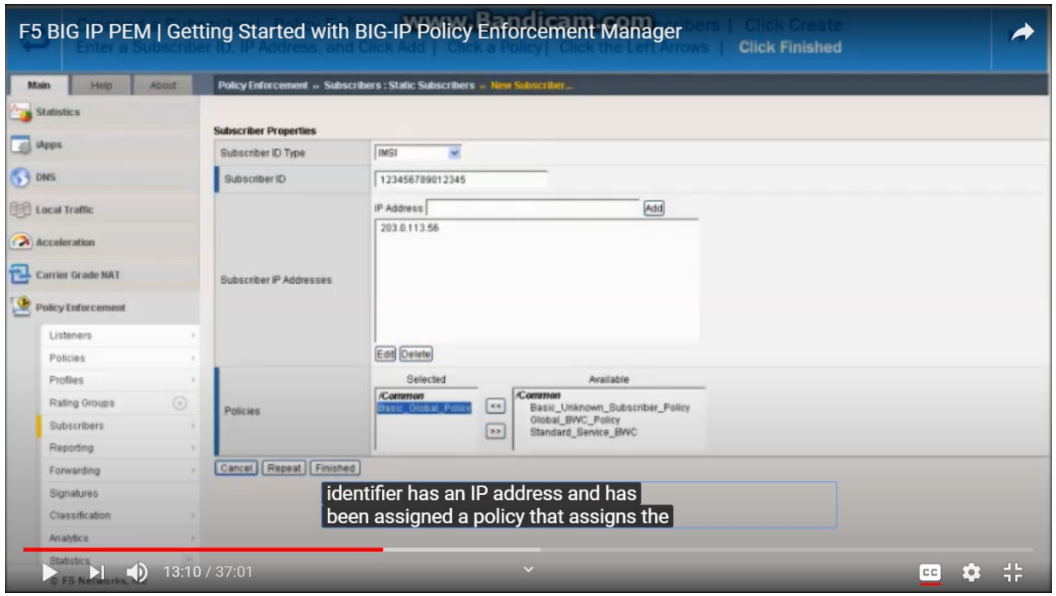
node, wherein at least two of the plurality of node-specific policies are different, and wherein the at least two node-specific policies are associated with respective at least two different nodes of the plurality of nodes.	rule or policy definition may include a set of one or more rules or policies. **In some embodiments, the classification of a packet is based at least in part on the group of rules that the packet matches or satisfies. For example, a packet may be compared against one or more rules in the set of rules defining an ingress network security policy, and the packets classification may be based at least in part on the rules that the packet matches or satisfies.** [Col. 6, Line 38-51] **The node-specific security policy of each node may be defined at**	**Citation 10: Policies assigned to the subscriber**  Fig. 10 Source: https://www.youtube.com/watch?v=HxzI2BKy_jg, Timestamp 13:10/37:01, Last accessed April 28, 2020, Exhibit B Fig. 11 shows different rule conditions to be met and different rule actions taken by the corresponding nodes.

Exhibit 2

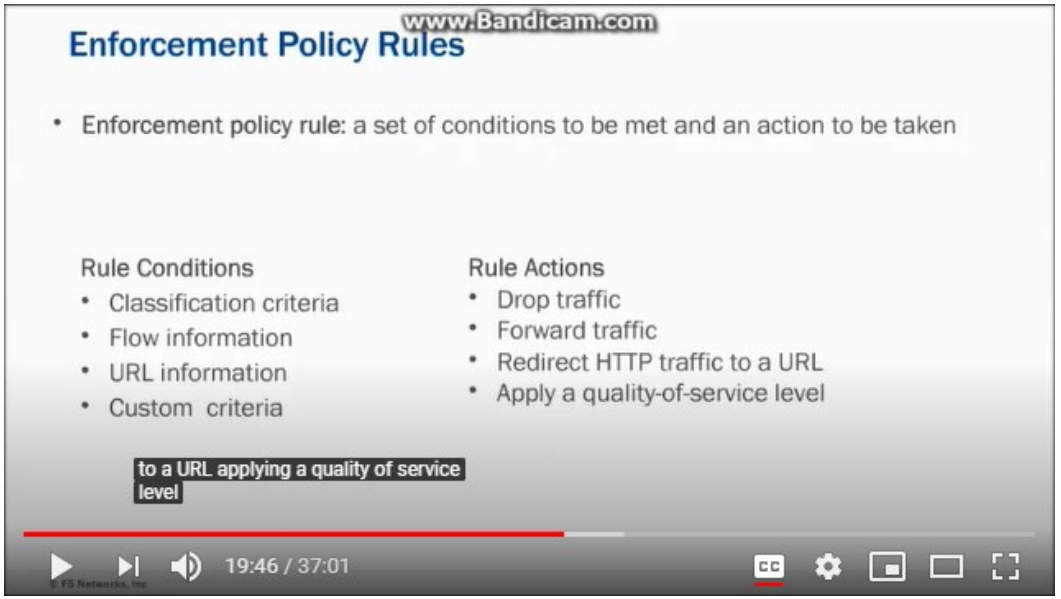
	least in part by the actions or processing to be performed by a node on different types of packets received by the node and may be stored in an appropriate data structure at each node. [Col. 7, Line 66 - Col. 8, Line 3]	**Citation 11: Enforcement Policy Rules**  Fig. 11 Source: https://www.youtube.com/watch?v=HxzI2BKy_jg, Timestamp 19:46/37:01, Last accessed April 28, 2020, Exhibit B Different policies are assigned to a subscriber, ultimately to the subscriber ID based on the user requirement (i.e., receiving node) E.g., one user may want higher bandwidth, while other user wants some parental control. (i.e., at least two of the plurality of node-specific policies are different). See Fig. 12.

Exhibit 2

		Citation 12: Different policies based on user requirement **Policy Enforcement** **Intelligent traffic steering** With BIG-IP PEM, service providers can perform layer 7 advanced steering of application and subscriber traffic to multiple, value-added services including web caching, video optimization, and parental control. For example, BIG-IP PEM detects if a subscriber's mobile device is consuming video. If so, it can direct traffic from that device to your video **Bandwidth control** BIG-IP PEM provides significant flexibility in controlling bandwidth—via rate limiting, DSCP marking, and layer 2 quality of service marking. Limits can be applied to a group of subscribers, to all subscribers, or at the application level. This flexibility enables you to establish tiered services to create and manage incremental revenue-generating plans based on subscribers' actual data usage patterns. Bandwidth control can also be used to implement fair-usage policies to allow your subscribers to consume a fair amount of bandwidth while distributing it more proportionally across the subscriber base. Fig. 12 Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 3, Last accessed September 4, 2020, Exhibit A Therefore, packets are mapped to a subscriber's identity (Subscriber ID) (i.e., classification index). Further processing on the packet is based on the subscriber's ID associated with it. As an example, 'Global_BWC_Policy' has been applied to the subscriber having ID as '123456789012345'. Whenever a packet for this subscriber arrives at the PEM, it will be mapped with the subscriber's ID, and further processing on the packet will be done based on rules defined in the policies

Exhibit 2

		associated with the subscriber. (i.e., node-specific policies associated with a plurality of nodes is specified using the classification data) See Fig. 13. **Citation 13: Applying a policy to a subscriber**  Fig. 13 Source: https://www.youtube.com/watch?v=HxzI2BKy_jg, Timestamp 36:13/37:01, Last accessed April 28, 2020, Exhibit B Fig. 14 shows different settings such as classification, URL, flow, etc., based on which a packet will be filtered.

Exhibit 2

Citation 14: Creating Policy – Settings on a packet filter

Fig. 14

Source: https://www.youtube.com/watch?v=HxzI2BKy_jg,Timestamp 22:14/37:01, Last accessed April 28, 2020, Exhibit B

By way of an example, the actions performed by the different nodes such as QoS node, Reporting node, etc. when the conditions are met are shown in Fig. 15.

Citation 15: Creating policy – performing actions

Exhibit 2

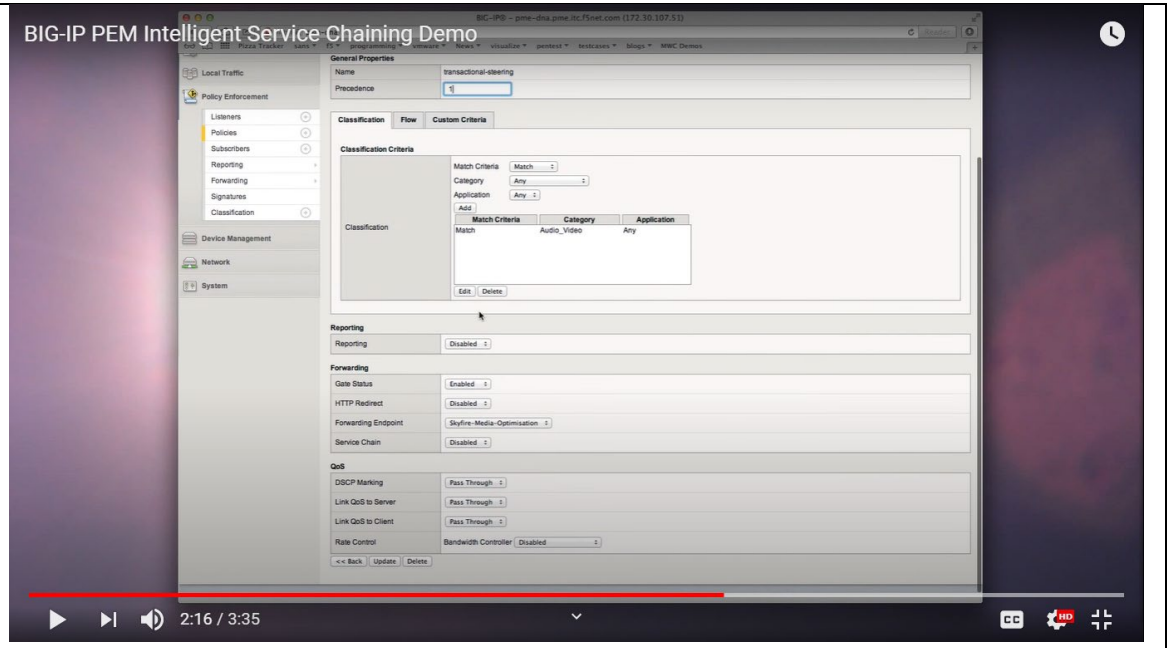


Fig. 15

Source: https://www.youtube.com/watch?v=Vs-rfLkVNTE, Timestamp 2:16/3:35, Last Accessed September 3, 2020, Exhibit E

Citation 16: Creating policy – Performing Actions

Exhibit 2

		 Fig. 16 Source: https://www.youtube.com/watch?v=HxzI2BKy_jg, Timestamp 22:27/37:01, Last accessed April 28, 2020, Exhibit B As different policies can be defined for different subscribers, every node (for taking necessary actions based on the policies) such as Reporting node, forwarding node, QoS node, etc. have different node-specific policies.

Exhibit 2

References Cited

Exhibit (s)	Description	Link
Exhibit A	F5 BIG-IP Policy Enforcement Manager (PEM) - Datasheet	https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf
Exhibit B	*Video Tutorial* - Getting Started with BIG-IP Policy Enforcement Manager	https://www.youtube.com/watch?v=HxzI2BKy_jg
Exhibit C	F5 Big IP Policy Enforcement Manager	https://www.f5.com/products/big-ip-services/policy-enforcement-manager
Exhibit D	F5 BIG-IP PEM Enforcement Policies	https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-13-0-0/1.html#guid-ee75a1d4-4c4d-4faf-a986-d22118411e0e,
Exhibit E	*Video* – BIG-IP Policy Configuration	https://www.youtube.com/watch?v=Vs-rfLkVNTE